IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PHILIP CAMACHO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

AMERICAN EXPRESS COMPANY,

Defendant.

Case No. 1:24-cv-02408-JPC

FIRST AMENDED CLASS ACTION COMPLAINT[1]

JURY TRIAL DEMANDED

Plaintiff Philip Camacho ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all California residents who applied for a credit card on Defendant American Express Company's ("Defendant" or "AmEx") website americanexpress.com (the "Website") and had their application rejected.

2. Defendant aided, employed, agreed, and conspired with Meta Platforms, Inc. ("Meta") to intercept communications sent and received by Plaintiff and Class Members. These include communications that include sensitive and confidential information, i.e., that Plaintiff applied for a credit card. By failing to procure consent before enabling Meta to intercept these communications, Defendant violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631 and 632.

[1] Plaintiff has obtained Defendant's written consent under Fed. R. Civ. P. 15(a)(2) to file this First Amended Complaint.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A) as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

4. This Court has personal jurisdiction over Defendant because Defendant's headquarters are in this District.

5. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant transacts business in this District and a substantial part of the events or omissions giving rise to the claim occurred in this District.

PARTIES

6. Plaintiff Camacho is, and has been at all relevant times, a resident of Chatsworth, California and has an intent to remain there, and is therefore a domiciliary of California. In or about March 2023, Plaintiff applied for an American Express credit card on Defendant's website, americanexpress.com. As part of the application on the Website, Plaintiff provided Defendant with multiple pieces of sensitive information, including but not limited to his name, phone number, his total annual income, and his income source. As described below, Defendant allowed the Facebook Tracking Pixel on the Website to send the fact that he applied for an American Express credit card contemporaneously to Meta. This information was intercepted in transit and sent to Meta without Plaintiff's knowledge, consent, or express written authorization. Defendant breached its duties of confidentiality and unlawfully eavesdropped upon Plaintiff and unlawfully

disclosed confidential information, namely, that Plaintiff applied for an American Express credit card.

7. Defendant American Express Company ("American Express") is a New York corporation with its principal place of business located in New York, New York. Defendant offers financial services throughout the United States, including in New York and California. American Express develops, owns, and operates americanexpress.com.

FACTUAL ALLEGATIONS

I. The California Invasion of Privacy Act

8. The California Legislature enacted the Invasion of Privacy Act to protect certain privacy rights of California citizens. The legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

9. The California Supreme Court has repeatedly stated an "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added)

10. Further, as the California Supreme Court has held in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*

> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Id., 38 Cal. 3d at 360-61 (emphasis added; internal citations omitted).

11. As part of CIPA, the California Legislature enacted § 631(a), which prohibits any person or entity from [i] "intentionally tap[ping], or mak[ing] any unauthorized connection … with any telegraph or telephone wire," [ii] "willfully and without the consent of all parties to the communication … read[ing], or attempt[ing] to read, or to learn the contents or meaning of any . . . communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [California]," or [iii] "us[ing], or attempt[ing] to use . . . any information so obtained."

12. CIPA § 631(a) also penalizes [iv] those who "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping, or those who "permit" the wiretapping.

13. As part of the Invasion of Privacy Act, the California Legislature additionally introduced Penal Code § 632(a), which prohibits any person or entity from "intentionally and without the consent of all parties to a confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or record [a] confidential communication."

14. A "confidential communication" for the purposes of CIPA § 632 is "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto." Cal. Penal Code § 632(c).

15. Individuals may bring an action against the violator of CIPA §§ 631 and 632 for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

II. The Facebook Tracking Pixel

16. Meta owns Facebook, the largest social networking site on the planet, touting 2.9 billion monthly active users. Facebook describes itself as a "real identity platform," meaning users are allowed only one account and must share "the name they go by in everyday life." To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.

17. Facebook generates revenue by selling advertising space on its website.

18. Facebook sells advertising space by highlighting its ability to target users. Facebook can target users so effectively because it surveils user activity both on and off its site. This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections." Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.

19. Advertisers can also build "Custom Audiences." Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website." Advertisers can use a Custom Audience to target existing customers directly, or they can use it to build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities." Unlike Core Audiences, Custom Audiences require an advertiser to supply the underlying data to Facebook. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," which collect and transmit the data automatically. One such Business Tool is the Facebook Tracking Pixel.

20. The Facebook Tracking Pixel is a piece of code that advertisers, like Defendant, can integrate into their websites, mobile applications, and servers, enabling Facebook to intercept and collect user information on those platforms. As the name implies, the Facebook Tracking Pixel "tracks the people and type of actions they take." When a user accesses a website hosting the Facebook Tracking Pixel, Facebook's software surreptitiously directs the user's browser to simultaneously send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Pixel collects. This transmission is initiated by Facebook code and is concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and a website: the website's own code, and Facebook's embedded code.

21. In other words, when a user communicates with Defendant's Website, those communications are simultaneously and contemporaneously duplicated and sent to Facebook at the same time as they are being sent to Defendant. Thus, Facebook's interception of these communications occurs "in transit."

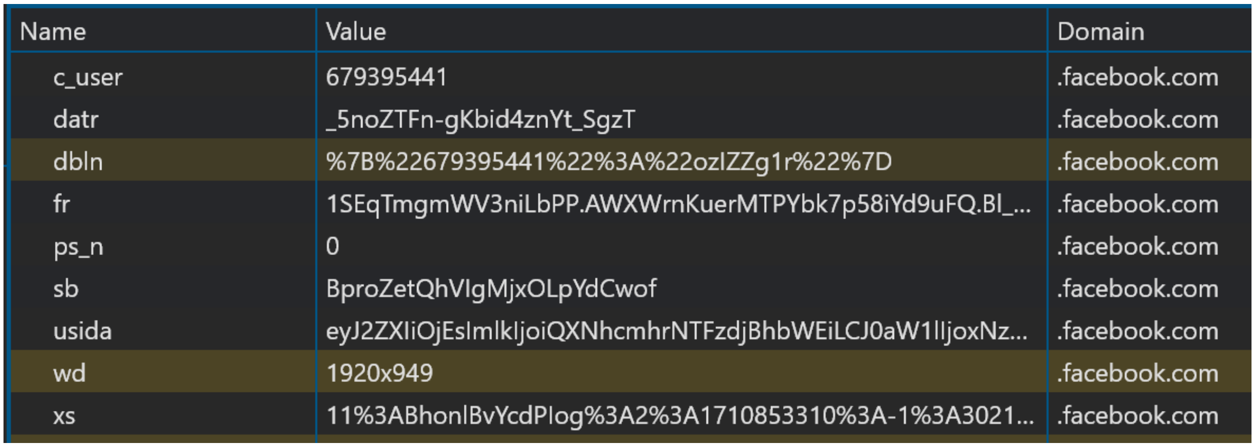
22. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

23. The Facebook Tracking Pixel tracks numerous types of action—or, as Facebook calls it, "events"—that users take on websites, including the website's metadata, along with what pages a visitor views and what buttons a visitor clicks. Events tracked through the Pixel include URLs visited and text typed into text boxes or fields, when Website users have progressed through portions of the Website (which requires affirmative button presses on the part of Website users), and many other items.

III. Use of the Facebook Tracking Pixel on Defendant's Website

24. Defendant provides credit card applications on its Website. Defendant has installed the Facebook Tracking Pixel on each webpage used for these applications.

25. Americanexpress.com contains the code for at least nine different Facebook cookies, including the c_user cookie, which transmits the user's Facebook ID:



Name	Value	Domain
c_user	679395441	.facebook.com
datr	_5noZTFn-gKbid4znYt_SgzT	.facebook.com
dbln	%7B%22679395441%22%3A%22ozIZZg1r%22%7D	.facebook.com
fr	1SEqTmgmWV3niLbPP.AWXWrnKuerMTPYbk7p58iYd9uFQ.Bl_...	.facebook.com
ps_n	0	.facebook.com
sb	BproZetQhVIgMjxOLpYdCwof	.facebook.com
usida	eyJ2ZXIiOjEslmlkIjoiQXNhcmhrNTFzdjBhbWEiLCJ0aW1lIjoxNz...	.facebook.com
wd	1920x949	.facebook.com
xs	11%3ABhonlBvYcdPlog%3A2%3A1710853310%3A-1%3A3021...	.facebook.com

26. When someone who is logged into Facebook applies for a credit card on americanexpress.com, as Plaintiff did, the Pixel transmits personally identifiable information from these Facebook cookies to Facebook along with their event data, including the fact that the particular user applied for an American Express credit card.

27. In addition, when a Website visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies, including the _fdp and fr cookies. No matter the circumstances, Facebook receives the fr cookie from a Website visitor's browser. The fr cookie contains, at minimum, an encrypted Facebook ID and browser identifier. The _fbp cookie contains, at least, an unencrypted value that uniquely identifies a browser. The datr cookies also identifies a browser. Facebook, at a minimum, uses the fr and _fbp cookies to identify users, and the fr, _fbp and c_user cookies to link to Facebook IDs and corresponding Facebook profiles.

28. A Facebook ID is personally identifiable information. Anyone can identify a Facebook profile—and all personal information publicly listed on that profile—by appending the Facebook ID to the end of facebook.com.

29. The combination of the event data and the personally identifiable information from Facebook's cookies embedded on americanexpress.com permits Facebook to obtain confidential information for specific individuals.

30. Defendant also uses these cookies to pair event data with confidential information and personally identifiable information so it can later retarget consumers on Facebook.

31. Furthermore, when Meta uses its wiretaps on Website users' communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. Instead, Meta, a separate and distinct entity, uses the wiretaps to eavesdrop upon, record, extract data from, and analyze conversations to which it is not a party. Meta itself collects the contents of said conversations and then analyzes that data.

32. Meta uses information it collects in this manner for purposes other than recording it and conveying it to Defendant, including but not limited to contact information matching; measurement and analytics services; ad targeting; commercial and transactional messages; ad delivery improvement; feature and content personalization; and product improvement, provision, and securement.

33. Meta does not collect data by accident. Meta has intentionally created and specially designed the Facebook Pixel for the express purpose of collecting individual user data from the websites (and other platforms) where users, including Plaintiff, transmit that information without knowing that their data is being collected, compiled, and analyzed by third parties, for purposes Plaintiff did not consent for it to be used.

34. To summarize the above allegations, Facebook, as enabled by Defendant, collects the contents of users' communications with the Website using the wiretaps described *supra*. These communications include the fact that a particular individual has applied for a credit card with American Express. This is information that is affirmatively entered by users on the Website. This information is not anonymized, because Defendant enables Facebook to link users' communications with personal identifiers (i.e., name, email address, Facebook ID, etc.), which reveal their identities.

35. Crucially, neither Defendant nor Facebook procures prior consent from users for Facebook to engage in this wiretapping. As alleged herein, Defendant allows for Facebook's collection of the fact that Website users have applied for an American Express credit card, even when Defendant has not received consent from Website users to do so.

36. Likewise, Facebook never receives consent from Website users to intercept and collect electronic communications containing their sensitive and unlawfully disclosed information. In fact, Facebook expressly warrants the opposite.

37. When first signing up for Facebook, a user assents to three agreements: the Facebook Terms of Service, the Cookies Policy, and the Privacy Policy. For California residents, Facebook also publishes a United States Regional Privacy Notice.

38. Facebook's Terms of Service begin by stating that "[p]rotecting people's privacy is central to how we've designed our ad system." The Terms of Service then prohibit anyone from using Facebook's Products in a manner that is "unlawful, misleading, discriminatory or fraudulent[.]"

39. Facebook's Privacy Policy describes how Facebook receives information like "[w]ebsites you visit and cookie data, like through Social Plugins or the Meta Pixel[,] . . . [h]ow

you use our partners' products and services, online or in person[,] . . . [and] information like your email address, cookies and advertising device ID[.]" Specifically, Facebook acknowledges that "[w]e collect and receive information from partners, . . . [and] receive this information whether or not you're logged in or have an account on our Products."

40. Facebook then offers an express representation: "We require partners to have the right to collect, use and share your information before giving it to us." Facebook also acknowledges collecting "information with special protections[,]" meaning information that "could have special protections under the laws of your jurisdiction[,]" but critically, only sensitive information that users "choose to provide."

41. Facebook's Cookies Policy ratifies those representations, stating "the Privacy Policy will apply to our processing of the data that we collect via cookies."

42. For California residents, Facebook reiterates that policy: "We require each of these partners to have rights to collect, use, and disclose your information before providing any information to us." The United States Regional Privacy Notice also restricts Facebook's ability to collect "sensitive personal information," stating they "will only use or disclose it either with your specific consent when required, or as otherwise permitted by law, including the CCPA."

43. Facebook's other representations reinforce these warranties. In its Advertising Policy, Facebook states "[w]e do not use sensitive personal data for ad targeting." And in a blog post titled "About Restricted Meta Business Tools Data," Facebook asserts it has "policies around the kinds of information businesses can share with us." Facebook does not "want websites or apps sending us certain restricted information about people." Sensitive information includes, among other things, "any information defined as sensitive under applicable laws, regulations and applicable industry guidelines."

44. These representations are repeated frequently. Facebook created a "Help Center" to better explain its practices to users. In an article titled, "How does Facebook receive information from other businesses and organizations?," Facebook reiterates its promise to "prohibit businesses or organizations from sharing sensitive information with us," and if Facebook "determine[s] that a business or an organization is violating our terms, we'll take action against that business or organization." In another article, titled, "How does Meta work with data providers?," Facebook repeats this promise, stating "[b]usinesses that advertise on Facebook are required to have any necessary rights and permissions to use this information, as outlined in our Custom Audience Terms that businesses must agree to."

45. A reasonable user who reads Facebook's terms and representations would understand those terms as requiring Facebook to enforce an advertiser's compliance with its terms. At a minimum, those terms and representations require Facebook to build safeguards for sensitive information. No reasonable user would read those terms and representations as permitting Facebook to intentionally intercept electronic communications that it knows the law protects and deems sensitive. In short, Facebook never receives consent from users to intentionally intercept and monetize electronic communications disclosing sensitive information that the law protects.

CLASS ALLEGATIONS

46. **Class Definition:** Plaintiff seeks to represent a class of similarly situated individuals defined as all persons in California with a Facebook account who applied for a credit card on americanexpress.com and had their application rejected (the "Class"). Subject to additional information obtained through further investigation and discovery, the above-described Class may be modified or narrowed as appropriate.

47. **Numerosity (Fed. R. Civ. P. 23(a)(1)):** At this time, Plaintiff does not know the exact number of members of the aforementioned Class. However, given the popularity of Defendant's website and credit cards, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

48. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2), 23(b)(3)):** There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

(a) whether Defendant disclosed Plaintiff's and the Class's confidential communications to Facebook;

(b) whether Defendant's disclosures were committed knowingly; and

(c) whether Defendant disclosed Plaintiff's and the Class's confidential communications without consent.

49. **Typicality (Fed. R. Civ. P. 23(a)(3)):** Plaintiff's claims are typical of those of the Class because Plaintiff, like all members of the Class, used Defendant's website to apply for a credit card, had his credit card application rejected, and had his confidential communications collected and disclosed by Defendant.

50. **Adequacy (Fed. R. Civ. P. 23(a)(4)):** Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation, including litigation concerning the Facebook Tracking Pixel and CIPA. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiff nor his counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims or the type reasonably expected to be raised by

members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this First Amended Class Action Complaint to include additional representatives to represent the Class, additional claims as may be appropriate, or to amend the definition of the Class to address any steps that Defendant took.

51. **Superiority (Fed. R. Civ. P. 23(b)(3)):** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Class is impracticable. Even if every member of the Class could afford to pursue individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action.

CAUSES OF ACTION

COUNT I
Violation Of The California Invasion Of Privacy Act
Cal. Penal Code § 631(a)

52. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

53. Plaintiff brings this claim against Defendant individually and on behalf of the Class.

54. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

55. CIPA § 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

56. Facebook's Business Tools, including but not limited to the Facebook Pixel, are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

57. Facebook is a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, as alleged herein, Facebook had the capability to use the wiretapped information for its own purposes, and the Pixel is software that allows a third party to capture messages in real time and later perform data analysis. Accordingly, Facebook was a third party to any communication between Plaintiff and Class Members, on the one hand, and Defendant, on the other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

58. At all relevant times, by its Business Tools, Facebook willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiff and Class Members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

59. At all relevant times, Facebook used or attempted to use the communications intercepted by its Business Tools to promote and improve its advertising platform

60. At all relevant times, Defendant aided, agreed with, employed, permitted, or otherwise enabled Facebook to wiretap Plaintiff and Class Members using the Business Tools and to accomplish the wrongful conduct at issue here.

61. Plaintiff and Class Members did not provide their prior consent to Facebook's intentional access, interception, reading, learning, recording, collection, and usage of Plaintiff's and Class Members' electronic communications. Nor did Plaintiff and Class Members provide

their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling Facebook's conduct.

62. The wiretapping of Plaintiff and Class Members occurred in California, where Plaintiff and Class Members accessed the Website and where Facebook—as enabled by Defendant—routed Plaintiff's and Class Members' electronic communications its servers.

63. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

COUNT II
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632

64. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

65. Plaintiff brings this claim against Defendant individually and on behalf of the Class.

66. CIPA § 632(a) prohibits an entity from:

> intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio.

67. Facebook's Business Tools, including but not limited to the Facebook Pixel, are software that surreptitiously intercepts personal data and communications and transmits this data Facebook. Accordingly, they are "electronic amplifying or recording device[s] " within the meaning of Cal. Pen. Code §632.

68. At all relevant times, Facebook intentionally used its Business Tools to eavesdrop upon and record the confidential communications of Plaintiff and Class Members, on the one hand, and Defendant, on the other.

69. Specifically, Plaintiff provided his personally identifiable financial information to Defendant in the course of his application for a credit card. The fact that Plaintiff applied for an American Express credit card is confidential information, and was collected through an Internet cookie or information collecting device. No reasonable person would expect the fact that they applied for an American Express credit card to be shared with an unknown third party.

70. When communicating with Defendant, Plaintiff and Class Members had an objectively reasonable expectation of privacy. Thus, Plaintiff and Class Members did not reasonably expect that anyone other than Defendant would be on the other end of the communication, and that a third-party, like Facebook, would intentionally use an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiff and Class Members.

71. Plaintiff and Class Members did not consent to any of Facebook's actions. Nor have Plaintiff or Class Members consented to Facebook's intentional use of an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff seeks a judgment against Defendant, individually and on behalf of all others similarly situated, as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) An award of statutory damages to the extent available;

(e) For punitive damages, as warranted, in an amount to be determined at trial;

(f) For prejudgment interest on all amounts awarded;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

(h) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b)(1), Plaintiff demands a trial by jury of all issues so triable.

Dated: September 11, 2024

Respectfully submitted,

By: *<u>/s/ Joshua D. Arisohn</u>*
Joshua D. Arisohn

BURSOR & FISHER, P.A.
Joshua D. Arisohn
Philip L. Fraietta
Alec M. Leslie
1330 Avenue of the Americas, 32nd Fl.
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: jarisohn@bursor.com
pfraietta@bursor.com
aleslie@bursor.com

Attorneys for Plaintiff